CPS DE E-CERTCHILE

Declaración de las Prácticas De Certificación

VERSIÓN 5.2
Fecha de Publicación: Junio de 2015
Requisito **PO02**

DECLARACIÓN DE LAS PRÁCTICAS DE CERTIFICACIÓN DE E-CERTCHILE

ÍNDICE

RESUMEN DE LOS DERECHOS Y OBLIGACIONES FUNDAMENTALES CONTENIDOS EN ESTA CPS

ESTE TEXTO ES UNA SÍNTESIS DEL CONTENIDO COMPLETO DE LA CPS. ACONSEJAMOS QUE LEAN SU TEXTO ÍNTEGRO Y LOS DEMÁS DOCUMENTOS AFINES PARA OBTENER UNA VISIÓN CLARA DE LOS OBJETIVOS, DERECHOS Y OBLIGACIONES QUE RIGEN EN LA RELACIÓN JURÍDICA CON E-CERTCHILE.

- Esta CPS y los documentos afines regulan todo lo relativo a la solicitud, emisión, aceptación, renovación, reemisión y revocación de certificados entre otros muchos aspectos vitales para la vida del Certificado y el régimen jurídico que se establece entre Solicitante/Suscriptor, E-CERTCHILE, los usuarios y terceros.

- Tanto la CPS como todos los demás documentos afines y complementarios son puestos a disposición de futuros Solicitantes, Suscriptores y Usuarios en la dirección de Internet http://www.E-CERTCHILE.cl para que conozcan exactamente, antes de contratar o confiar en E-CERTCHILE, cuáles son las normas y reglas aplicables a nuestro sistema de certificación.

- E-CERTCHILE emite varios tipos de certificados, por lo que el Solicitante de un Certificado deberá conocer las condiciones establecidas en la CPS y en las correspondientes Prácticas de Certificación Específicas de ese tipo de Certificado, de manera que pueda proceder correctamente a la solicitud y uso del Certificado.

- Es imprescindible la custodia de las claves privadas que el Suscriptor debe hacer respecto de su Certificado. En este sentido, es necesario realizar la petición de revocación como propietario del Certificado o bien informar inmediatamente a E-CERTCHILE cuando concurra alguna causa de revocación del Certificado establecidas en la CPS y proceder, de esta manera, a su revocación para evitar un uso ilegitimo del Certificado por parte de un tercero no autorizado.

- El Suscriptor debe hacer un uso debido del Certificado, y será exclusiva responsabilidad suya la utilización del Certificado de forma diferente a los usos previstos en la CPS y los demás documentos afines.

- Es obligación ineludible del Usuario comprobar bien en el Repositorio de Certificados publicados por E-CERTCHILE que el Certificado en el que pretende confiar es válido y no ha caducado o ha sido revocado.

- En la CPS y documentos afines se establece la responsabilidad de E-CERTCHILE y de los Solicitantes, Suscriptores y Usuarios, así como la limitación de la misma ante la posible producción de daños y prejuicios.

Para más información, consulte nuestra página Web en la dirección http://www.E-CERTCHILE.cl o póngase en contacto con nosotros a través de la siguiente dirección de e-mail: sclientes@E-CERTCHILE.cl

1. INTRODUCCIÓN

1.1 Presentación

El presente documento constituye el Estatuto de Prácticas de Certificación (Certificate Practice Statement) del servicio de certificación de E-CERTCHILE al cual se hará referencia mediante el acrónimo de su denominación en inglés CPS.

La presente CPS, junto con las Políticas de Certificación (CP) para cada tipo de Certificado, recogen las políticas que, la Empresa Nacional de Certificación Electrónica, actuando como Entidad de Certificación Digital bajo la marca E-CERTCHILE, empleará en la expedición de sus Certificados.

1.2 Identificación

El presente documento se denomina “Declaración de las Prácticas de Certificación de E-CERTCHILE” y puede localizarse en la siguiente dirección:
http://www.e-certchile.cl

1.3 Comunidad de Usuarios y Aplicaciones

Los Certificados de Firma Electrónica Avanzada permiten que las personas puedan firmar electrónicamente transacciones y documentación de esta clase. Identifica al usuario de forma única y podrá utilizarse en aquellas aplicaciones que precisen firma electrónica mediante certificados digitales X.509 v3 emitidos bajo la Política Firma Electrónica Avanzada. Este certificado permitirá sólo firmar de acuerdo a lo establecido en la ley 19.799 y su reglamento.
El suscriptor de este tipo de Certificados podrá ser cualquier persona natural, siempre que conforme a los criterios establecidos en la presente Práctica de Certificación (CPS) y la Ley 19.799 y su reglamento, solicite un certificado de FEA o de FEA con autenticación clase 5.
Firma y no Repudio
El receptor de un mensaje firmado con el Certificado puede usar la clave pública del emisor para verificar que este último ha usado su clave privada para suscribir el mensaje. El servicio de no repudio permite confirmar frente a un tercero la identidad del emisor del mensaje y la no alteración del mismo.
El mensaje firmado puede corresponder a una transacción y documento electrónico con validez legal según la legislación vigente, en especial la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
Integridad
El uso de los servicios de FEA y de FEA con autenticación clase 5 permite asegurar al receptor de un mensaje que éste no ha sido alterado entre el envío y la recepción.

1.3.1 Entidad de Certificación

E-CERTCHILE actúa como Entidad de Certificación (PSC) relacionando una determinada clave pública con un sujeto o entidad concretos a través de la emisión de un Certificado de conformidad con los términos de esta CPS.

1.3.2 Entidad de Registro

Corresponde a una entidad intermedia entre la Entidad de Certificación (EC) y los Solicitantes, que se encarga de la detección, comercialización y administración de las solicitudes de certificación. Se encarga de establecer, confirmar y registrar las identidades y los antecedentes y atributos de los usuarios finales sujetos a certificar. La EC podrá valerse de una o varias Entidades de Registro (ER), elegidas libremente, sin perjuicio de que éstas deberán llevar a cabo el proceso de comprobación fehaciente de la identidad del Solicitante conforme a estas.

1.3.3 Suscriptor

El Suscriptor del Certificado podrá ser aquel que se derive de las Políticas de Certificación (CP) para presentar la solicitud de un Certificado.

1.3.4 Solicitante

A los efectos de esta CPS, se entenderá por Solicitante a la persona natural autorizada por cada una de las Políticas de Certificación para presentar la solicitud de un Certificado.

1.3.5 Usuarios

Se entiende por Usuario del Certificado a la persona que voluntariamente confía y hace uso de los Certificados de E-CERTCHILE.

Cuando el Usuario decida voluntariamente confiar y hacer uso del Certificado le será de aplicación la presente CPS.

1.3.6 Tipos de Certificados

Los distintos tipos de certificados que se ofrecen dentro del ámbito de esta CPS están definidos en cada una de sus respectivas POLÍTICAS DE CERTIFICACIÓN (CP). Cada una de las CP regula la aplicabilidad de un certificado en relación a una

comunidad de usuarios y algunos usos y restricciones determinados con requerimientos de seguridad comunes.

1.3.7 Limitaciones de Uso

Los usos autorizados de los Certificados emitidos por la PSC vienen especificados en cada una de las Políticas de Certificación correspondientes a cada tipo de Certificado.
Se deja constancia de que los certificados no son medios de pago, sino que su finalidad es identificar a una persona en un sistema de redes abiertas o cerradas. No obstante, los certificados regidos por esta CPS pueden ser utilizados en operaciones que importen órdenes de pago o transferencias de dinero.
Estos Certificados son válidos para asumir las responsabilidades económicas y compromisos en nombre propio permitidos por la Ley 19.799 y en general serán válidos para los usos descritos en este documento.
No se permite un uso del Certificado contrario a:

- La normativa chilena y a los convenios internacionales ratificados por el Estado Chileno.

- Lo establecido en la CPS, en la Política de Certificación y en los contratos que se firmen entre la EC (Entidad de Certificación) / ER (Entidad de Registro) y el Suscriptor.

Los certificados de E-CERTCHILE no podrán ser alterados, deberán utilizarse tal y como son suministrados por la EC.

1.4 Detalles de Contacto

Atención.: Solicitud Clientes
E-CERTCHILE
Monjitas 392 Piso 17
Santiago de Chile

E-mail: sclientes@E-CERTCHILE.cl
Teléfono: 56-2-23607152
Horario de Atención: Mesa ayuda certificación: - Fono: (02)28185760
Mesa ayuda certificación: - Horario atención: 09:00 - 18:30 hrs. de lunes a viernes
Horario atención en nuestras oficinas: 09:00 - 17:30 hrs. de lunes a viernes

2 CONDICIONES GENERALES

2.1 Obligaciones

2.1.1 Obligaciones de la PSC

Obligaciones de E-CERTCHILE, como prestadora de servicios de certificación son todas aquellas obligaciones impuestas por la presente CPS y en especial las siguientes:

- Asegurar conformidad de sus procesos y actividades con las prácticas de certificación definidas en este documento y las respectiva CP para cada tipo de certificado.
- Emitir certificados haciendo uso de tecnologías y criptografía que permitan un adecuado proceso de certificación.
- Apoyar la emisión de certificados con las tecnologías que permitan el resguardo de las llaves privadas en posesión de E-CERTCHILE.
- Mantener registro de certificados y su estado actualizado, para consulta de usuarios.

Frente a los Suscriptores:

- Notificar al Suscriptor de la emisión de su Certificado.
- Notificar al Suscriptor de la revocación de su Certificado.
- Mantener actualizados los registros de certificados vigentes y certificados revocados.
- Revocar certificados que no cumplan con declaraciones de las CPS o de la CP correspondiente al tipo de certificado.
- Transmitir las soluciones de revocación de certificados de forma oportuna.
- Efectuar los estudios e informes de poderes de los Solicitantes/Suscriptores personas jurídicas con apoderados.

Frente a los Usuarios:

- Asegurarse de que toda la información incluida o incorporada por referencia en el Certificado es exacta, salvo que se declare expresamente en el Certificado, o en la CPS, que no ha sido verificada o confirmada.
- Cumplir de manera sustancial con el contenido de esta CPS.
- Poner a disposición de los usuarios los certificados que componen la(s) cadena(s) de certificación de E-CERTCHILE.

2.1.2 Obligaciones de ER

La ER podrá asumir las siguientes obligaciones de las cuales será responsable.

- Identificar y autenticar correctamente al Suscriptor y/o Solicitante y/o a la organización que represente, conforme a los procedimientos que se establece en esta CPS y en las Políticas de Certificación para cada tipo de Certificado, utilizando cualquiera de los medios admitidos en derecho.

- Enviar información fidedigna y previamente validada de los suscriptores, para efectos de certificación.

- Formalizar los contactos de expedición de Certificados con Suscriptor en los términos y condiciones que establezca la PSC.

- Mantener y garantizar existencia de registro electrónico de los antecedentes de los suscriptores.

- Almacenar de forma segura y por un período razonable la documentación aportada en el proceso de emisión del Certificado y en el proceso de revocación del mismo.

- Llevar a cabo cualesquiera otras funciones que le correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta CPS.

- Aplicar medidas de seguridades adecuadas y suficientes para salvaguardar su llave privada.

En todo caso, la ER permitirá a la PSC el acceso a los archivos y a los procedimientos de conservación de los archivos asumidos por la ER y le dará el derecho a investigar cualquier sospecha de infracción de la CPS y/o de las Políticas de Certificación por parte de la ER o cualquier poseedor de un Certificado. La ER y los poseedores de cualquier Certificado deberán informar a la PSC inmediatamente de cualquier sospecha de infracción.

Todas las funciones atribuidas a la ER, siempre y cuando no exista colisión con los derechos reconocidos a estas mediante acuerdos individuales, podrán ser desempeñadas de forma directa por parte de la PSC, en cuyo caso toda referencia de esta CPS a una ER deberá entenderse hecha a la PSC.

2.1.3 Obligaciones del Solicitante

- Solicitar el Certificado según se estipula en la CPS, las Políticas de Certificación (CP) y en atención a las instrucciones de E-CERTCHILE (solamente a través del sitio web de E-CERTCHILE www.E-CERTCHILE.cl).

- Proveer de la totalidad de los antecedentes requeridos y de las facilidades necesarias para la realización de las validaciones correspondientes.

2.1.4 Obligaciones del Suscriptor

- Conservar y utilizar correctamente el Certificado.

- Custodiar el Certificado, de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación de clave privada, modificación o uso no autorizado.

- Proteger mediante password la importación y utilización del Certificado cuando este se almacene en disco local del PC, y mediante el PIN en caso de que el Certificado esté soportado en un dispositivo portable seguro (por ejemplo Tarjeta Inteligente o E-Token) que cumpla con los estándares establecidos para la emisión de dicho certificado.

- Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos previstos en el epígrafe titulado “REVOCACIÓN DE CERTIFICADOS” de la presente CPS.

- No revelar la clave privada ni el código de activación del Certificado.

- Asegurarse de que toda la información contenida en el Certificado es correcta y notificar inmediatamente a la ER o PSC, según corresponda. Para el Certificado de Firma Digital Avanzada solamente la PSC es la entidad autorizada, por lo tanto todo lo relacionado y que se mencione en esta CPS, con el Certificado de Firma Digital Avanzada debe ser informado a través de los medios de comunicación definidos en la CP establecida para dicha certificado, ya sea por Mail, vía telefónica o Acto presencial en las dependencias de E-CERTCHILE Monjitas 392 Piso 6, en atención a Servicio al Cliente, en el horario establecido para ello es de 8:30 hrs. a 18:00 hrs. solo se atenderá en días hábiles. En caso de que se haya incluido cualquier información incorrecta o inexacta o en caso de que, de forma sobrevenida, la información del Certificado no corresponda con la realidad. De considerarlo necesario, podrá comunicar los cambios o variaciones que haya sufrido cualquiera de los datos que aportó para adquirir el Certificado, aunque éstos

no estuvieran incluidos en el propio Certificado (tales como domicilio, Nº de teléfono, etc.).

- Informar inmediatamente a la ER o la PSC acerca de cualquier situación que pueda afectar a la validez del Certificado.

- Destruir el Certificado cuando así lo exija la PSC o la ER en virtud del derecho de propiedad que en todo caso conserva sobre el Certificado, cuando el Certificado caduque o sea revocado.

- Realizar un uso debido y correcto del Certificado, según se desprende de esta CPS y de las Prácticas de Certificación. Será responsabilidad del Suscriptor el uso indebido que éste haga del mismo.

- Cualquier otra que se derive de la ley, del contenido de esta CPS o de las Políticas de Certificación.

2.1.5 Obligaciones de los Usuarios

Los usuarios que pretendan confiar y usar los Certificados emitidos por la PSC deberán verificar la validez de las firmas emitidas por los Suscriptores.

En el supuesto de que los Usuarios no procedieran a verificar las firmas a través de la CRL (Lista de Certificados revocados), Servicio de Consulta Web, o eventualmente a través de una EV (Entidad de Validación), la PSC no se hace responsable del uso y confianza que los Usuarios hagan de estos Certificados.

2.1.5.1 Confianza de las firmas

Toda persona tendrá derecho a confiar en una firma electrónica emitida mediante un Certificado E-CERTCHILE en la medida en que sea razonable hacerlo.

Para determinar si es razonable confiar, deberá tenerse en cuenta, en su caso lo siguiente:

1) La naturaleza de la operación correspondiente que la firma tenga por objeto avalar. No se considerará razonable confiar en una firma emitida por un Certificado E-CERTCHILE si dicha operación puede ser considerada ilícita.

2) Si la parte que confía ha adoptado las medidas adecuadas para determinar la fiabilidad de la firma, y en particular, si ha verificado que el Certificado usado para firmar era confiable al momento de firmar.

3) Si la parte que confía sabia o debía haber sabido que la firma estaba en entredicho o había sido revocada.

4) Las políticas y procedimientos que rijan la actividad de E-CERTCHILE con relación a las firmas emitidas mediante certificados por ella emitidos y se especifican en su CPS y en cada una de las Políticas de Certificación emitidas para cada tipo de Certificado.

5) Todo otro factor pertinente.

2.1.5.2 Confianza en los Certificados

Toda persona tendrá derecho a confiar en un Certificado E-CERTCHILE en la medida en que sea razonable hacerlo.

Para determinar si es razonable confiar, deberá tenerse en cuenta, en su caso, lo siguiente:

1) Toda restricción a que esté sujeto el Certificado;

2) Si la parte que confía ha adoptado las medidas adecuadas para determinar la caducidad o estado de revocación del Certificado,

3) Las políticas y procedimientos que rijan la actividad de E-CERTCHILE con relación a las firmas emitidas mediante certificados por ella emitidos y que se especifican en su CPS y en cada una de las Políticas de Certificación (CP) emitidas para cada tipo de Certificado.

4) Todo otro factor pertinente.

Los usuarios del servicio de certificación E-CERTCHILE se obligan a conocer y aceptar los términos, condiciones y límites contenidos en esta CPS y en las Políticas de Certificación, dentro de los cuales se asegura la prestación de los servicios de certificación.

2.2 Responsabilidad

2.2.1 Responsabilidad de la PSC

La PSC no será responsable de los daños derivados o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del Solicitante, Suscriptor y/o Usuario.

La PSC no será responsable de la incorrecta utilización de los Certificados de FEA ni de los FEA con autenticación clase 5 ni de cualquier daño indirecto que pueda resultar de su uso.

Tratándose de la FEA con autenticación clase 5, la EC garantiza que los datos de creación de firma no son accesibles a través de un sistema diferente al bioelectrónico acordado y disponible, por lo que será especialmente responsable de cualquier activación que se produzca de los mismos, siempre que culminen con la suscripción de una transacción o documento, con un sistema diferente al bioelectrónico acordado y disponible.

La PSC no será responsable de las eventuales inexactitudes en el Certificado de FEA ni de la FEA con autenticación clase 5 que resulten de la información facilitada por el Suscriptor a la ER, a condición de haber actuado siempre con la máxima diligencia exigible.

La PSC no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud de la presente CPS si tal falta de ejecución o retraso resultara o fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia sobre la que la PSC no pueda tener un control razonable y entre otros: Los desastres naturales, la guerra, el estado de sitio, las alteraciones de orden público, la huelga en los transportes, el corte de suministro eléctrico y/o telefónico, los virus informáticos, deficiencias en los servicios de telecomunicaciones.

La complejidad de los sistemas informáticos y el propio riesgo tecnológico hace imposible garantizar que no existan errores o inconsistencias en el sistema, no obstante el cuidado y la diligencia puesta por la PSC. Por ello, no se proporciona ninguna garantía en relación al posible compromiso en el futuro del sistema de claves asimétricas o cualquier otro riesgo no predecible de análoga naturaleza. Con la finalidad de mitigar esta clase de riegos la PSC deberá aplicar los procedimientos previstos en sus planes de contingencia.

Será responsabilidad de los usuarios adoptar las prevenciones usuales en computación para evitar daños y prejuicios originados por el uso o incapacidad de uso de los Certificados de FEA o de FEA con autenticación clase 5.

La EC no será responsable del contenido de los documentos suscritos electrónicamente mediante un Certificado de FEA o de FEA con autenticación clase 5.

Cualquiera que sea la causa por la que pudiera reclamarse responsabilidad a la EC o la ER, la pretensión indemnizatoria no podrá exceder, salvo en el supuesto de culpa grave o dolo, la cantidad de 360 UF.

2.2.2 Responsabilidad de la ER

La ER responderá de las funciones que le correspondan conforme a esta CPS y, en especial, asumirá toda la responsabilidad por la correcta identificación y validación del Solicitante/Suscriptor, con las mismas limitaciones que se establecen en el apartado anterior con relación a la PSC.

2.2.3 Responsabilidad del Suscriptor

El Suscriptor se compromete a indemnizar a la PSC los daños o perjuicios que puedan ocasionar cualquier acto u omisión culposo o doloso por su parte, asumiendo igualmente los gastos judiciales en que la PSC pudiera incurrir por esta causa, incluyendo las costas de abogados y procuradores.

2.2.4 Responsabilidad del Usuario

En todo caso, el Usuario asumirá toda la responsabilidad y riesgos derivados de la aceptación de un Certificado sin haber realizado previamente la preceptiva verificación de su validez, garantizando la plena indemnidad de la PSC por dicho concepto.

2.3 Responsabilidad Financiera

Las responsabilidades que afectan la operación de E-CERTCHILE están establecidas y limitadas a lo establecido en el artículo 14 de la Ley 19.799.

2.3.1Indemnización de parte de los Suscriptores y las Partes que Confían

2.3.1.1 Indemnización de parte de los Suscriptores

No aplica.

2.3.1.2 Indemnización de las Partes que Confían

No Aplica.

2.4.2 Procesos Administrativos

Los Clientes de E-CERTCHILE contarán con los recursos financieros suficientes para mantener sus operaciones y llevar a cabo sus deberes, y deben ser razonablemente capaces de soportar el riesgo de la responsabilidad para con los Suscriptores y las Partes que Confían. Los Clientes de E-CERTCHILE también mantendrán un nivel comercialmente razonable de cobertura de seguro por los errores y omisiones, ya sea a través de un programa de seguro de errores y omisiones con una aseguradora o una retención para auto asegurados. Esta exigencia de seguro no se aplica a las entidades gubernamentales. E-CERTCHILE mantiene dicha cobertura de seguro de errores y omisiones.

2.4 Interpretación y Ejecución

2.3.1 Ley aplicable

El presente documento y las Prácticas de Certificación específicas para cada tipo de Certificado se regirán por la Ley chilena, con arreglo a la cual deberá ser interpretado su contenido.

2.3.2 Subrogación, Novación y Notificaciones

La PSC se reserva el derecho de transmitir en el futuro todas las obligaciones y derechos que se deriven de esta CPS a un tercero para que éste continúe prestando el servicio de certificación. En este caso, la PSC notificará este extremo a los Suscriptores cuyos Certificados estén en vigor con una antelación mínima de dos meses, los cuales son conscientes y aceptan esta posibilidad. Esta CPS seguirá siendo el documento que regule las relaciones entre las partes mientras no se cree un nuevo documento por escrito.

La PSC podrá modificar cualquiera de las cláusulas de la presente CPS en los términos previstos en esta CPS.

2.3.3 Procedimiento de Resolución de Conflictos

Para la resolución de cualquier conflicto que surgiese en relación a esta CPS o a la CP correspondiente al tipo de certificado, las partes involucradas, se someterán al arbitraje de un arbitrador. El árbitro se designará por acuerdo común de ambas partes, con un plazo máximo de 15 días hábiles, a contar de lo cual el caso pasará a manos de la justicia ordinaria.

2.3.4 Tasas de Registro por la Expedición y Renovación de Certificados.

El costo por la emisión o renovación de los Certificados serán puestas a disposición de los Solicitantes por cada ER. Estas últimas podrán, dentro del área en el que presten sus servicios, establecer promociones especiales, ofertas o similares que modifiquen las tarifas previamente establecidas.

2.4 Publicación y Depósito de la CPS

El contenido de esta CPS, así como de toda la información que se publique, estará expuesta a título informativo en la dirección de Internet: http://www.E-CERTCHILE.cl y los originales estarán depositados en las oficinas de la PSC.

Igualmente, tanto los Usuarios como los Solicitantes/Suscriptores podrán tener acceso de forma fiable a la información de la PSC dirigiéndose a sus oficinas o a las de cualquier ER, o bien, solicitándolo a la dirección sclientes@E-CERTCHILE.cl a través de la cual se remitirá la información firmada con un Certificado de E-CERTCHILE.

2.5 Confidencialidad y Protección de Datos

2.5.1. Confidencialidad de las Claves de Firma Digital

Las claves de firma criptográfica privada no son generadas por E-CERTCHILE sino que mediante la funcionalidad provista por el Proveedor de Servicios de Criptografía (Cryptographic Service Provider) PSC, disponibles en sistema del cliente. Por esta razón, la PSC y la ER no conocen ni disponen de respaldo de las llaves privadas de los certificados generados.

En la FEA con autenticación clase 5 las claves de firma criptográfica privada serán generadas por E-CERTCHILE mediante la funcionalidad provista por el Proveedor de Servicios de Criptografía (Cryptographic Service Provider) PSC, serán almacenadas en un módulo criptográfico FIPS 140-2 y se podrá acceder a ellas únicamente mediante el sistema bioelectrónico, acordado y disponible, que asegura que los datos de creación de firma se mantienen bajo el exclusivo control del suscriptor.

2.5.2 Confidencialidad en la Prestación de Servicios de Certificación

Tanto la PSC como la ER mantendrán la más estricta confidencialidad de toda información recibida de parte de los Solicitantes y Suscriptores de Certificados, siempre que la publicación o comunicación a terceros de dicha información sea necesaria para la correcta prestación de los servicios de certificación. La PSC

solicitará la autorización del Solicitante y Suscriptores cuando precise utilizar los datos para otros fines.

2.5.3 Protección de Datos

Se deja constancia de la existencia de una base de datos con la información obtenida de los procesos de solicitud y registro del solicitante de los servicios de Certificación según se estipula en la CPS y en las Políticas de Certificación. La base de datos es responsabilidad de la Empresa Nacional de Certificación Electrónica S.A. o cualquier entidad que se subrogue para llevar a cabo la prestación y gestión de los servicios de Certificación prestados por E-CERTCHILE. El envío de los formularios y la firma de los contratos implicará el consentimiento expreso del titular para la cesión de sus datos de carácter personal contenidos en la referida base de datos a las ER que formen parte de la red E-CERTCHILE, así como a todos los Usuarios del sistema E-CERTCHILE en la medida en que sea necesario para llevar las acciones previstas en la CPS y las Prácticas de Certificación y para realizar las labores de información y comercialización. El responsable de la base de datos se compromete a guardar secreto respecto a los datos contenidos en ésta de acuerdo con la legislación aplicable al efecto. Asimismo, se le informa de su derecho de acceso, rectificación, cancelación y, en su caso, oposición de acuerdo con lo establecido en la Ley 19.628 sobre Protección de la Vida Privada y demás normativa aplicable.

2.5.4 Tipos de Información que debe mantenerse Confidencial y Privada

Los siguientes registros de Suscriptores, sujetos al artículo 2.8.2 de la CPS, se mantienen confidenciales y privados (“Información Confidencial/Privada”):

- Registros de Solicitudes de Certificado (sujetas al artículo 2.8.2 de la CPS),
- Registros de Transacciones (tanto registros completos como el rastreo de auditorías de transacciones);
- Registros de rastreo de auditorías de E-CERTCHILE que crea o retiene;
- Los informes de auditoría creados por E-CERTCHILE o sus auditores respectivos (ya sean internos o públicos).
- Planeación de contingencia y planes de recuperación de desastres, y Medidas de seguridad que controlan las operaciones del hardware y software de E-CERTCHILE y la administración de servicios de Certificados y los servicios de inscripción designados.

2.5.5 Tipos de Información que no se considera Confidencial ni Privada

E-CERTCHILE declara que los Certificados de FEA y FEA con autenticación clase 5, la revocación de Certificados y la información contenida en ellos no se consideran Información Confidencial/Privada. Asimismo, se establece que dicha información es tratada de conformidad con el artículo 12 b) de la Ley 19.799.

2.6 Derechos de Propiedad Intelectual

La PSC es titular de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta CPS. Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de la PSC sin la autorización expresa por su parte. No obstante, no necesitará autorización de la PSC para la reproducción del Certificado cuando la misma sea necesaria para la utilización del Certificado por parte del usuario legítimo y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta CPS.

3 IDENTIFICACIÓN Y AUTENTICACIÓN

Debido a que E-CERTCHILE maneja políticas con diferentes métodos de registro y autenticación, este apartado se desarrolla para cada tipo de Certificación a través de las CP específicas de cada política

3.1 Registro Inicial

3.1.1 Tipos de Nombres

Los Certificados de la EC de E-CERTCHILE están basado en la estructura x509 v3 que contiene los datos expresados en notación DN (Distinguished Name), donde un DN se compone a su vez de diversos campos. Los DN correspondientes al campo SUJETO y ASUNTO de E-CERTCHILE consiste en los elementos que se especifican en el Cuadro siguiente.

Atributo	Valor
País (C) =	"CL"
Organización (O) =	E-CERTCHILE
Unidad Organizacional (UO) =	Autoridad Certificadora
Estado o provincia (S) =	Región Metropolitana
Localidad (L) =	Santiago
Dirección de correo electrónico (E) =	email@E-CERTCHILE.cl
Nombre Común (CN) =	E-CERTCHILE CA

Cuadro – Atributos del DN en los Certificados de la EC

Los Certificados del Suscriptor usuario final también contiene los datos expresados en notación DN (Distinguished Name) en los campos del SUJETO y ASUNTO y contienen los elementos que se especifican en el cuadro siguiente.

Atributo	*Valor*
País (P) =	"CL"
Organización (O) =	El atributo de la organización se usa como sigue: • El nombre de la empresa del Suscriptor
Unidad Organizacional (UO) =	• Puede contener el departamento organizacional al que pertenece el suscriptor, por ejemplo Gerencia
Estado o Provincia (S) =	Indica el Estado o Provincia o Región
Localidad (L) =	Indica la Ciudad del Suscriptor
Nombre Común (CN) =	Este atributo comprende: • Nombre (para los Certificados Individuales)
Dirección de correo electrónico (E) =	Dirección de correo electrónico para los Certificados
Limitaciones	Contiene las limitaciones temporales y de funcionalidad del certificado expresando que se trata de certificados cuya vigencia alcanza a un acto de firma

Cuadro – Atributos del DN en los Certificados del Suscriptor Usuario Final

El elemento de Nombre Común (CN=) del DN del Sujeto de los Certificados del Suscriptor usuario final se autentica cuando se trata de los Certificados Clase 3 como es la de FEA o de Clase 5 como es la FEA con autenticación clase 5.

El valor del nombre común autenticado que se incluye en los DN del Sujeto del Certificado organizacional es el nombre legal de la organización o unidad dentro de la organización.

- El valor del nombre común que se incluye en el nombre distinguido del Sujeto de los Certificados individuales representa el nombre de la persona natural.

3.1.2 Necesidad de que los Nombres sean Significativos

Los Certificados del Suscriptor usuario final contienen nombres de persona natural y que permite la determinación de la identidad de la persona que es el Sujeto del Certificado. No se permiten los seudónimos de los Suscriptores usuarios finales (nombres que no sean el nombre verdadero personal) en esos Certificados.

Los certificados de la EC de E-CERTCHILE contienen nombres con semántica que se entiende comúnmente y permite la determinación de la identidad de la EC que es el Sujeto del Certificado.

3.1.3 Singularidad de los Nombres

E-CERTCHILE garantiza que los DN del Sujeto son únicos dentro del dominio de una EC específica a través de elementos del proceso de inscripción del Suscriptor.

3.1.4 Procedimiento de Resolución de Conflictos por Reclamaciones de Nombres

No aplica.

3.1.5 Reconocimiento, Autenticación y Papel de las Marcas Registradas

No aplica

3.1.6 Método para comprobar la Posesión de la Clave Privada (datos de creación de firma)

E-CERTCHILE implementará un sistema de eliminación de las claves privadas (datos de creación de firma) una vez que se cumpla la condición de término de vigencia del certificado, entregando al suscriptor los antecedentes necesarios para la comprobación de la inutilización del certificado una vez producida su extinción.

3.1.7 Autenticación de la Identidad de la Organización

E-CERTCHILE comprueba la información de la organización ingresada por el solicitante del certificado para efectos de facturación servicios de certificación y para los efectos de la incorporación de la información en el Certificado cuando se requiera la notación en el campo Organización y Unidad Organizacional.

3.2 Regeneración Rutinaria de Nueva Clave de Certificado

No Aplica.

3.2.1 Reposición de la Clave y Renovación de Rutina para los Certificados del Suscriptor Usuario Final

No Aplica.

3.3 Reposición de la Clave después de la Revocación

No aplica.

3.4 Solicitud de Certificado

3.4.1 Registro Inicial

El Solicitante deberá llenar el formulario dispuesto por la entidad de registro para la solicitud del Certificado. El ingreso de los datos solicitados en este formulario supondrá su consentimiento para ser registrado como Solicitante de un Certificado E-CERTCHILE de FEA o FEA con autenticación clase 5. La solicitud de este certificado no implicará en ningún caso su obtención del mismo si no llegan a cumplirse por parte del solicitante las cláusulas y condiciones establecidos en la

CPS, en la Política de Certificación para los Certificados de Firma Electrónica Avanzada y en el Contrato del Suscriptor con la EC.

En el mismo acto el solicitante proporcionará a la ER toda la información que necesite, bien para registrar al Solicitante como Suscriptor, o con la finalidad de incluirla en el Certificado, de acuerdo con los requisitos establecidos en esta CPS.

3.4.2 Autenticación de la Identidad del Suscriptor

Para que la ER compruebe fehacientemente la identidad del solicitante, el solicitante deberá acreditar todas las menciones básicas del certificado, para lo cual deberá presentar los siguientes documentos:

- Cédula Nacional de Identidad o Pasaporte si fuera extranjero, ambos vigentes.
- Tratándose de la FEA en que se vayan a incluir antecedentes en el campo Organización y Unidad Organizacional, si se solicita, los documentos acreditativos de tales calidades.

3.4.3 Confirmación de la Identidad del Suscriptor

Una vez recibida la solicitud, la ER procederá a la aprobación de la misma, previo proceso de verificación de la información proporcionada, según lo indicado en el correo de aceptación.

En concreto, la ER confirmará: la identidad de la persona, mediante presentación de documento de identidad válido y la correspondencia con este antecedente de los datos biométricos proporcionados por el solicitante, lo cual se verificará contra una base de datos biométrica de confianza, a efecto de proceder a la validación de los datos necesarios para la creación de los datos de creación de firma.

3.4.4 Aceptación de la Solicitud

Una4 vez superado el proceso de comprobación de solicitud de forma satisfactoria, siempre y cuando no existan circunstancias que de alguna manera afecten a la seguridad del servicio de certificación, la ER procederá a la aprobación de la solicitud.

3.4.5 Rechazo de la Solicitud

Si la ER decidiese rechazar la solicitud del Certificado, comunicará presencialmente y por escrito al Solicitante dicha decisión. Este rechazo en ningún caso implica que el Solicitante no pueda requerir posteriormente éste u otro servicio de E-CERTCHILE.

3.5 Emisión de Certificado

Una vez aceptada por la ER la Solicitud del Certificado, se llevará a cabo el registro del solicitante.

Prerrequisitos
- Entrega de la documentación requerida y que ésta sea correcta y completa.
- Exhibir Cédula de Identidad o Pasaporte si fuera extranjero, vigente

El Certificado y su contenido son propiedad de la EC y se emitirá con carácter personal e intransferible a nombre del suscriptor. La ER se obliga a:

a) La ER verificará la identidad del solicitante de la FEA o de la FEA con autenticación clase 5 a través de los procedimientos definidos en este numeral.

b) E-certchile puede utilizar otros mecanismos automáticos e inequívocos de validación de identidad, como por ejemplo el uso de la huella dactilar que incorpora la lectura de esta por medios electrónicos y validación a través de repositorios de datos validados.

c) La ER deberá solicitar el número del formulario de enrolamiento. El respaldo digital del mismo será guardado en un directorio de acceso restringido y respaldado semanalmente.

d) El operador ER, deberá solicitar la firma al Suscriptor y contrato de utilización de sistema bioelectrónico como medio de creación de firma. El respaldo digital del mismo será guardado en un directorio de acceso restringido y respaldado semanalmente.

e) El operador ER, deberá registrar y validar con el sistema biométrico, acordado y disponible, que asegura que los datos de creación de firma se mantienen bajo el exclusivo control del titular del certificado.

f) El Operador ER, generará y enviará electrónicamente, a través de sesión segura, la solicitud a la EC para que proceda a la emisión del certificado y a almacenar las claves privadas en el módulo criptográfico FIPS 141-2, especialmente habilitado, para que almacene las claves a las que sólo podrá acceder el titular de las mismas mediante clave.

Caso de Excepción:
Si se efectúa exitosamente el registro del suscriptor, pero por algún motivo, no es posible emitir el certificado de forma inmediata, el proceso de certificación terminará y la ER y la EC procederá a la eliminación de toda información relacionada con el Suscriptor del Certificado y que se haya

recabado con ocasión de este proceso de emisión de certificado de FEA con autenticación clase 5.

El suscriptor se obliga a:

a) Dar cuenta de cualquier irregularidad que detecte en el sistema
b) Presentar su carnet de identidad válido y vigente
c) Seguir correctamente el proceso solicitado por el operador ER para la emisión del certificado
d) Revocar en caso de extravío o pérdida.

La EC se reserva el derecho a negarse a emitir Certificados cuando concurra cualquier causa justificada, por lo que no podrá exigírsele responsabilidad alguna por este motivo.

3.6 Aceptación del Certificado

3.6.1 Aceptación del Certificado por parte del Suscriptor

La entrega del Certificado, la firma, el estampado de huella dactilar en Formulario de Enrolamiento y la firma contrato de adhesión al sistema de Certificación implicará la aceptación del Certificado por parte del suscriptor. De forma bioelectrónica
La aceptación del Certificado deberá realizarse de forma expresa, por escrito y ante el encargado de la ER.
El suscriptor deberá firmar original y copia del contrato, estableciendo su total aceptación al servicio de certificación que se le ha otorgado. La copia del contrato perteneciente al suscriptor será entregada personalmente al suscriptor o despachada por correo certificado al domicilio que éste haya declarado en la fase de registro.
Aceptando el Certificado, el suscriptor confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que de ello se derive frente a la ER, la EC o cualquier tercero que de buena fe confíe en el contenido del Certificado.

3.6.2 Publicación del Certificado

Una vez aceptado el Certificado por parte del suscriptor, la EC procederá a la publicación, en el Registro de Acceso Público.
La publicación de los datos del Certificado en el Registro de Acceso Público significa que ha sido aceptado para los terceros usuarios de buena fe, que confíen en el Certificado.

3.6.3 Contenido del Certificado

Versión x509 v3

3.6.4 Perfil de Certificado de la Política de Firma Electrónica Avanzada

Versión	3	
Serial Number	0202AF	
Signature algorithm	md5RSA	
Issuer	Pais	C=CL
	Organización	O=E-CERTCHILE
	Unidad Organizacional	OU=Empresa Nacional de Certificación Electrónica
	Nombre	CN=E-CERTCHILE CA Intermedia
	Localidad (ciudad)	L=Santiago
	Estado (región)	S=Region Metropolitana
Valid from	Dayname, Month day, year hh:m:ss PM/AM	
Valid to	Dayname, Month day, year hh:m:ss PM/AM	
Subject	Pais	C=CL
	Email	E=mail@algundomino.cl
	Organización	O=Particular
	Estado (Region)	S=Region Metropolitana
	Nombre	CN=nombres apellido1 apellido2
	Localidad (Ciudad)	L=Santiago
	Unidad Organizacional	OU=Particular
Public Key	RSA (2048 Bits)	
EXTENSIONES		
Subject Alternative Name	Rut del suscriptor, OID: 1.3.6.1.4.1.8321.1	
CRL Ditributions Points	URL=http://crl.E-CERTCHILE.cl/ecertchilecaFEA.crl	
Issuer Alternative Name	Rut de EC emisora, OID: 1.3.6.1.4.1.8321.2	
Authority Key Identifier	KeyID=3710 CADF FD46 2285 C9E8 9EE6 1DD8 9CEF 00B6 AE50	
Certificate Policies	http://www.E-CERTCHILE.cl/html/productos/download/CPSv1.8.pdf	
Key Usage	Digital Signature	
Basic Constraints (Critica)	Subject Type=End Entity Path Length Constraint=None	

PROPIEDADES	
Thumbprint algorithm	Sha1
Thumbprint	
Algoritmo de firma	md5withRSAEncryption, OID:1 2 840 113549 1 1 4
Algoritmo de huella digital	SHA1

Nota: DN = Distinguished Name

4 REVOCACIÓN DE CERTIFICADOS

La revocación de Certificados son mecanismos a utilizar en el supuesto de que por alguna causa establecida en la presente CPS se deje de confiar en el Certificado antes de la finalización de su período de validez originalmente previsto.

4.1 Supuesto de Revocación

Los Certificados deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

- Solicitud voluntaria del Suscriptor.
- Pérdida o inutilización por daños del soporte del Certificado.
- Fallecimiento del signatario o de su representado, incapacidad sobreviviente, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.
- Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
- Inexactitudes graves en los datos aportados por el signatario para la obtención del Certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.
- Que se detecte que las claves privadas del Suscriptor o de la PSC han sido comprometidas, bien por que concurran las causas de pérdida, robo, hurto,

modificación, divulgación o revelación de las claves privadas, bien por cualquiera otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.

- Por incumplimiento por parte de la ER, PSC o el Suscriptor de las obligaciones establecidas en esta CPS.

- Por la resolución del contrato tal y como esta se regula en la presente CPS.

- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.

- Por resolución judicial o administrativa que lo ordene conforme a derecho.

- Por la concurrencia de cualquier otra causa especificada en la presente CPS o en las correspondientes CP establecidas para cada tipo de Certificado.

4.1.1 Efectos de la Revocación

El efecto de la revocación del Certificado es la pérdida de fiabilidad del mismo, originando el cese permanente de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La revocación de un Certificado impide el uso legítimo del mismo por parte del Suscriptor.

La revocación del Certificado por causa no imputable al Suscriptor originará la emisión de un nuevo Certificado a favor del Suscriptor por el plazo equivalente al restante para concluir el periodo originario de validez del Certificado revocado.

La revocación del Certificado tendrá como consecuencia la notificación a terceros de que un Certificado ha sido revocado, cuando se solicite la verificación del mismo.

4.2 Procedimiento de Revocación.

4.2.1 Legitimación Activa

Deberán solicitar la revocación en cuanto tengan conocimiento de la concurrencia de alguna de las circunstancias contempladas en el apartado 4.1 anterior:

- El Suscriptor del Certificado así como la persona natural o jurídica representada por éste.

- La ER, respecto a aquellos Certificados en cuya emisión hayan participado.
- La persona jurídica que conste en el Certificado.

Asimismo, podrá solicitar la revocación cualquier tercero con un interés legítimo en caso de que tenga conocimiento de la existencia alguna de las siguientes causas:

- Pérdida del soporte del Certificado.
- Fallecimiento del signatario.
- Incapacidad sobreviviente, total o parcial.
- Inexactitudes en el Certificado.
- Compromiso de la fiabilidad del Certificado.
- Compromiso de las claves.
- Cese del representante en el caso de los certificados con poderes.
- Extinción de la persona jurídica representada.
- Revocación de la autorización de la entidad que conste en el Certificado en el caso de los Certificados sin poderes.

En todo caso, la PSC podrá iniciar de oficio el procedimiento de revocación de Certificados, en cualquiera de los casos previstos en el apartado 4.1 anterior.

4.2.2 Recepción de Solicitudes de Revocación

Se establece el siguiente procedimiento para la solicitud de revocación de un Certificado:

a) Notificación de la revocación, identificándose e indicando los motivos, por medio de uno de los siguientes mecanismos:
   - Comunicación telefónica a través del siguiente número: 56 2 23607152
   - Vía e-mail: sclientes@E-CERTCHILE.cl
   - Vía Web en la dirección: http://www.E-CERTCHILE.cl

Sólo el Suscriptor del certificado puede utilizar alguno de los medios anteriores, en el caso de que fuera otra persona el solicitante, deberá concurrir personalmente a la oficina de E-CERTCHILE para realizar su solicitud.

En el caso de que la solicitud sea realizada por alguno de los medios detallados en el apartado anterior, E-CERTCHILE procederá a **Revocar** el certificado, a la espera de su ratificación.

El Suscriptor (o un usuario) dispone de 48 horas desde su solicitud para presentarse ante E-CERTCHILE para ratificar su solicitud de Suspensión/Revocación. El Suscriptor deberá presentar su RUT para identificarse y se le hará entrega del formulario de ratificación de revocación de certificado, en donde se debe señalar el motivo de revocación debe ser firmado y estampada su huella dactilar.

b) Mediante la presencia física del usuario en la ER donde realizó la solicitud del Certificado, ratificando la revocación.

Cualquiera sea el mecanismo utilizado para solicitar la revocación, el suscriptor deberá aportar como datos de identificación el set de claves utilizados para descargar el certificado y el número de serie de éste. En caso de carecer de los anteriores datos, se validará la identidad del suscriptor previo a dar cuerpo a la revocación del certificado. Si la causa es por fallecimiento del suscriptor, se validará la información del obituario oficial. Cualquier otra forma no contemplada será resuelta por la ER o PSC.

El inicio del proceso de revocación se realizará en forma inmediata al ser recibida la solicitud.

Cuando la persona que solicita la revocación del Certificado no sea el propio Suscriptor, deberá dirigirse en persona a cualquiera de las oficinas de la PSC o las ER.

Las conversaciones telefónicas que se mantengan podrán ser grabadas y registradas por E-CERTCHILE a efectos probatorios.

4.2.3 Decisión de Revocar

Una vez recibida y autenticada la solicitud de revocación, E-CERTCHILE efectuará la revocación efectiva del Certificado. La decisión de revocar un Certificado corresponde a la EC.

4.2.4 Comunicación y Publicación de la Revocación

La decisión de revocar el Certificado será comunicada por la PSC al Suscriptor mediante e-mail firmado digitalmente, y en el caso de solicitar la revocación vía Web la confirmación le será desplegada automáticamente indicando el código de revocación.

Igualmente, se publicará la revocación del Certificado en la CRL.

La revocación comenzará a producir efectos a partir de su publicación por parte de la PSC, salvo que la causa de revocación sea el cese de la actividad de la PSC, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

5 CADUCIDAD DE CERTIFICADOS

Los Certificados caducarán por el transcurso del período operacional del mismo.

La caducidad producirá automáticamente la invalidez del Certificado, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La caducidad de un Certificado impide el uso legítimo del mismo por parte del Suscriptor.

6 RENOVACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN

6.1 Renovación de Certificados

Este procedimiento se establece para los casos en que el Certificado vaya a caducar y el Suscriptor simplemente desee utilizar un Certificado con las mismas características que tenía el que venía utilizando válidamente hasta entonces.

En este caso, la PSC emitirá un nuevo Certificado y se generarán nuevas claves.
Es requerido llevar a cabo nuevamente el proceso de verificación y validación de la identidad del suscriptor.

Los Certificados emitidos por E-CERTCHILE tienen un plazo de vigencia de un año. Se podrá acudir a los trámites que se establecen en este documento para la renovación de los servicios de certificación de E-CERTCHILE si concurren los extremos generales que a continuación se detallan.

6.1.1 Requisitos Previos

Deberán concurrir los siguientes:

- Que el suscriptor posea o hubiese poseído en el anterior periodo, un certificado emitido por E-CERTCHILE.
- Que el Suscriptor desee la renovación del servicio de certificación que lo solicite en debido tiempo y forma, siguiendo las instrucciones y normas que E-CERTCHILE específica a tal efecto.
- Que la PSC no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación del Certificado.
- Que el Suscriptor se someta a los trámites correspondientes para la emisión de un Certificado como cualquier otro Solicitante que solicita su Certificado por primera vez.
- Que la solicitud de renovación de servicios de prestación se refiere al mismo tipo de Certificado emitido inicialmente.

6.1.2 Cómo Solicitar la Renovación

El Suscriptor que solicite la renovación de los servicios de certificación deberá completar un formulario que se encontrará a su disposición en la dirección de Internet: http://www.E-CERTCHILE.cl/
El Suscriptor enviará ese formulario debidamente llenado a la PSC. El Suscriptor titular de un Certificado se someterá al régimen general de solicitud de emisión de Certificado, esta consiste en la emisión de un nuevo certificado que ha perdido vigencia o se encuentra próximo a perderla. Luego de lo cual se continuará con el mismo proceso ocupado para registro y emisión de nuevos certificados. El certificado que ha perdido vigencia no es necesario revocarlo debido a que por restricciones de fecha no puede continuarse su uso.

6.1.3 Procedimiento de Renovación de Certificados

Cuando la PSC reciba la solicitud del Suscriptor en debida forma, procederá con el mismo proceso ocupado para registro y emisión de nuevos certificados.

La PSC emitirá el certificado solicitado, esta acción activará el envío de un e-mail al Solicitante el cual le notificará que el Certificado puede ser descargado de la dirección de Internet http://www.E-CERTCHILE.cl Este e-mail contendrá la clave para activar su Certificado, además de la descripción del proceso de descarga este proceso no opera para el Certificado de Firma Digital Avanzada.

Con la renovación de los servicios de certificación se entenderán que se mantienen los derechos, obligaciones y responsabilidades tanto de Suscriptor como de PSC y

ER, según se establece en los correspondientes contratos, la CPS y de las Políticas de Certificación aplicables.

6.2 Reemisión de Certificados

Este procedimiento se establece para los casos en que el Certificado de un Suscriptor sea declarado revocado por la existencia de exactitudes en el Certificado.

6.2.1 Requisitos Previos

Se podrá acudir a los trámites que se establecen en este documento para la reemisión de certificados de E-CERTCHILE si concurren a la vez los requisitos generales que a continuación se detallan:

- La solicitud la debe llevar a cabo el Suscriptor del antiguo Certificado.
- El origen de la solicitud debe basarse en la renovación del Certificado por inexactitudes en el mismo.
- En caso de revocación por inexactitudes, el plazo para poder solicitar la reemisión será de 15 días a contar desde la fecha en que le fuera notificada la resolución de revocación.
- La solicitud debe realizarse en debida forma, siguiendo las instrucciones y normas que E-CERTCHILE específica a tal efecto.
- La solicitud de reemisión del Certificado debe referirse al mismo tipo de Certificado emitido inicialmente.

6.2.2 Cómo Solicitar la Reemisión

El antiguo Suscriptor que solicite la reemisión de los servicios de certificación deberá llenar un formulario que se encontrará a su disposición en la dirección de Internet: http://www.E-CERTCHILE.cl.

El Suscriptor deberá manifestar en dicho formulario, bajo su responsabilidad, cuáles de los datos que constaban en su Certificado ya revocado no son ciertos o han variado de alguna forma.

La ER revisará la validez formal de la solicitud de reemisión y enviará a la PSC una solicitud para la creación de un nuevo Certificado a nombre del Suscriptor. A continuación, la propia ER PSC, se pondrá en contacto con el Suscriptor para realizar el cotejo de la identidad y de los datos del Certificado que hayan variado

según la resolución de revocación y/o la declaración del Suscriptor, solicitando la presencia física de éste último y requiriendo la exhibición de cuantos documentos originales considere necesarios.

Para la validación definitiva de los nuevos datos del Certificado, y para la entrega de éste, se aplicará el mismo procedimiento que para la primera emisión, aunque únicamente se procederá a comprobar aquellos datos cuya modificación haya sido aclarada.

6.2.3 Procedimiento de Reemisión de Certificados

Una vez presentada la documentación necesaria, la ER examinará si procede o no la reemisión del Certificado, distinguiendo tres supuestos:

a) Defectos subsanables en la presentación. En este caso, la ER deberá comunicar al Solicitante tal error o defecto, otorgándole un plazo de 15 días para subsanarlo. Si transcurriera tal plazo sin que el antiguo Suscriptor lo subsanara, éste deberá realizar todos trámites por los que solicita la emisión del Certificado por primera vez como cualquier otro Solicitante que no tenga un Certificado anterior. Si el Solicitante sí subsanara los defectos en los que había incurrido, el procedimiento se regirá según se estipula en el apartado c) establecido más adelante.

b) Defectos no subsanables en la presentación. En este supuesto la ER notificará al antiguo Suscriptor que solicita la reemisión estas circunstancias, denegándole la posibilidad de reemisión del Certificado.

c) La documentación presentada es la necesaria y concurren los requisitos exigibles. En este caso, la ER entregará al Suscriptor el nuevo Certificado, entendiéndose que se mantienen los derechos, obligaciones y responsabilidades tanto del Suscriptor como de PSC y ER, según se establece en los correspondientes contratos, la CPS y de las Políticas de Certificación aplicables.

7 EXTINCIÓN DE LA PSC

En orden a causar el menor daño posible tanto en los Suscriptores como a los Usuarios del sistema de certificación ante una hipotética desaparición de la PSC se establecen las siguientes medidas:

- Comunicar la extinción mediante el envío de un correo electrónico Certificado o una notificación mediante correo ordinario Certificado dirigido a todos los Suscriptores cuyos certificados permanezcan en vigor y la publicación de un

anuncio en dos diarios de tirada nacional. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

- Establecer, cuando ello fuera posible, acuerdo con terceras personas con la intención de transmitir todas sus obligaciones y derechos dentro del sistema de certificación con la intención de continuar el servicio. Si se produce la subrogación, a la cual el Suscriptor da su consentimiento de manera expresa, esta CPS seguirá siendo el documento que establece las relaciones entre las partes mientras no se establezca un nuevo documento por escrito.

- Proceder, en caso de no haberse podido llevar a cabo transferencia de derechos y obligaciones a otra entidad, a la revocación de todos los Certificados una vez transcurrido el plazo de dos meses desde la comunicación.

- Indemnizar adecuadamente a aquellos Suscriptores que lo soliciten cuando sus Certificados sean revocados con anterioridad al plazo previsto de vigencia, pactándose como tope para la indemnización el coste efectivo del servicio, descontando a prorrata el coste por los días transcurridos desde el inicio del contrato hasta la fecha de resolución.

- Cualquier otra obligación que venga impuesta por la ley.

8 CONTROLES DE SEGURIDAD

Con el objeto de reforzar la seguridad técnica, física, de procedimientos y de capacitación del personal, la PSC dispone de un reglamento interno de funcionamiento que regula todos estos aspectos.

Los requerimientos básicos de seguridad que ha de observar la PSC son los siguientes:

- El software y la información de la PSC correrá en una estación de trabajo dedicada a tal fin, Con las providencias y medidas necesarias para protegerlo contra ataques de la red interna y por sobre todo de la red externa.

- La clave de firma de la PSC tendrá una longitud de 2048 bits.

- Al menos una copia de los Backups del equipo de la PSC podrán deberán ser instalados en instalaciones externas a la PSC.

9 AUDITORIAS

Los procedimientos y frecuencia para la realización de auditorías de seguridad técnica, física, de procedimientos y de capacitación del personal, están regulados en el reglamento interno de la PSC.

10 CARACTERISTICAS DE LOS CERTIFICADOS Y DE LAS LISTAS DE CERTIFICADOS

10.1 Características del Certificado

Los certificados podrán ser emitidos en diversos tipos de soportes, siempre que estos se ajusten a las Políticas de Certificación: Tarjetas inteligentes, e-token, disco local, etc... Las tarjetas serán emitidas únicamente en las instalaciones donde se ubica la PSC y la ER.

Los Certificados tendrán una validez de un año a partir de su fecha de validez inicial.

10.2 Listas de Certificados Emitidos por E-CERTCHILE

Los certificados una vez emitidos se publicarán en una base de datos o repositorio disponible públicamente. Esta operación será realizada por personal autorizado a partir de los ficheros generados por la PSC.

Los certificados revocados por la PSC serán publicados en un repositorio disponible públicamente. Esta operación será realizada por personal autorizado a partir de los ficheros generados por la PSC.

El Listado de Certificados revocados (CRL) estará a disposición de los usuarios en la página web de la PSC:

http://crl.E-CERTCHILE.cl/ecertchilecaFEA.crl

Los Usuarios de Certificados pueden consultar en cualquier momento el estado de un Certificado determinado, por lo siguientes mecanismos:

Visitando la página Web de publicación de la CRL
Realizando consultas en línea mediante la Entidad de Validación
Realizando la solicitud correspondiente a través del siguiente número de teléfono: 56 2 23607152

11 ADMINISTRACION DE ESPECIFICACIONES

11.1 Procedimiento de Modificación de la CPS y de las CP

La PSC podrá modificar las estipulaciones de la presente CPS y de su CP específicas, sin prejuicio de que se mantenga el nivel de calidad esencial de sus servicios de certificación y, siempre y cuando, toda modificación se justifique desde el punto de vista jurídico, técnico y comercial.

11.2 Procedimiento de Publicación de las modificaciones

Las modificaciones efectuadas sobre la CPS o las CP se darán a conocer a los interesados en la página Web de PSC http://www.E-CERTCHILE.cl/ y en las oficinas de la PSC y de la ER.

A estos efectos, en dicha página Web, se hará una referencia expresa y fácilmente localizable a la existencia de dicha modificación, durante un período de treinta días.

De igual modo, se procederá a sustituir la versión anterior de la CPS o de las CP por la nueva.

En la página Web de la PSC se incluirá un listado de control de las sucesivas versiones que sobre la CPS o las CP puedan originarse, desde el que se podrá tener acceso tanto a la versión actual y operativa como a las versiones anteriores con una antigüedad no superior a un año.

11.3 Procedimiento de Notificación de las Publicaciones

En caso que las modificaciones efectuadas en la CPS o en las Políticas de Certificación incidan directamente en los derechos y obligaciones de los Suscriptores y/o Solicitantes, así como cuando dichas modificaciones alteren la operatividad de los Certificados por parte de los usuarios, deberán notificarse dichas modificaciones a los Suscriptores y/o Solicitantes con un período de antelación de quince días a la aplicación de los cambios efectuados.

El transcurso de dicho período sin que medie comunicación escrita por parte del Suscriptor y/o Solicitante, en contra de las citadas modificaciones implicará su aceptación. La no aceptación de las modificaciones de esta CPS o de las Políticas de Certificación realizadas por la PSC, tendrá como consecuencia la resolución de contrato con el Suscriptor/Solicitante.

Se considerará como medio eficaz para la realización de notificaciones el correo electrónico firmado digitalmente y enviado a la dirección proporcionada por el Suscriptor y/o Solicitante.

12 REFERENCIAS

La presente CPS está basada principalmente en la propuesta de estándar para la redacción de políticas y prácticas de certificación, del grupo de trabajo del IETF PKIX.

**** FIN DEL DOCUMENTO ****

Anexo Revisión

Versión	Fecha	Revisión	Observaciones
1.0	24/01/2003	1.0	Primer documento.
2.0	01/11/2010	2.0	Segundo documento
3.0	01/11/2011	3.0	Tercer documento
4.0	01/10/2012	4.0	Cuarto documento
5.0	01/04/2013	5.0	Quinto documento
5.1	01/06/2013	5.1	Sexto documento

Elaborado por Comité de Seguridad de la Información Consultora de Seguridad de la Información	Fecha: 01 de noviembre de 2010
Revisado por: Comité de Seguridad de la Información	Fecha: 01 de noviembre de 2010
Autorizador por: Gerente General E-certchile	Fecha: 01 de noviembre de 2010
Autorizador por: Comité de Seguridad de la Información	Fecha: 01 de Octubre de 2012
Publicado	Fecha: 01 de Octubre de 2012
Modificado	Fecha: Abril de 2013
Representante legal 1	Carlos Astudillo
Representante legal 2	Domingo Beas
Oficial de Seguridad	Domingo Teneos
Subgerente de operaciones y Tecnología	Patricio Díaz
Jefe Operaciones PKI	Priscila Pérez